

Digital Resilience Checklist for Action

As we action together as a movement, we want to make sure our folks are practicing collective care as physical, digital, and legal attacks escalate against our community. We are here for each other and committed to our safety as we pursue justice for our people. One of the most important things we can do is to take the time to know the people we are working with, use that network to vet new folks, talk about security with each other, and have clear agreements about security practices that are based in power rather than paranoia.

BEFORE AN ACTION

Stepping up in this moment means we need to practice protective measures to defend ourselves against attacks on our physical and digital selves. The recommendations here are not to drive your expression underground, but rather to **keep your private life separated from your public political self**.

We have to defend ourselves from both aggressive law enforcement efforts to criminalize our movement, as well as white nationalist trolls. **Trolls** are users - white supremacists, neo-Nazis, anti-Muslim bigots, anti-immigrant, anti-vaxxers, men's rights activists and others are active in dubious underground forums like 4chan and in Discord groups which most justice-centered organizers would never visit. . They actively organize online "raids" to target individual activists for harassment, intimidation, and sometimes even physical attacks.

Additionally, law enforcement in every locale actively monitors information shared on platforms like Facebook, Twitter, Instagram, and WhatsApp so as to both infiltrate and inform their activities. Sometimes, in certain cities, white supremacist trolls and law enforcement work in tandem.

One of the main techniques of the trolls is "doxxing" or collecting private information like home addresses in order to harass organizers and protestors. Here are some ways in which you can maximize your safety.

1. **Make your connections/friends, photos, groups and likes on social media private.** Make sure you do this on all publicly accessible platforms, including LinkedIn and Facebook. Your Facebook profile and cover photo will always be public, so choose wisely
2. **Minimize where your phone number, email address, home address or family members are publicly listed.** While this can be difficult to do, audit your social media accounts for places where these details can be leaked.
3. **Be careful about visibility on Facebook** events, groups, and pages. If you are RSVPing, make sure that you are not publicly visible.
4. **Use a virtual phone number in organizing. NEVER expose your real phone number.** You can use a free phone number Google Voice. If you have disposable funds, consider investing in a

commercial app like Burner App, CoverMe or Hushed. These tools will not protect you from law enforcement investigations, but could shield you from trolls and white supremacists.

5. **Use a free tutanota.com email address for organizing purposes and, if possible, use a VPN to access this.** This is necessary so that your IP address is not logged as you use it. It is also particularly important if you use these email addresses in list servers or for other activities. **TOR** is also excellent as a replacement browser.
6. **Do not use your real name and personal email address on online petitions.** Online petitions are often harvested and then used for political targeting and doxxing campaigns against our members. You can avoid this by aliasing your name and email address.
7. **Use Signal groups for organizing purposes.** Signal Messenger continues to be the gold standard for organizing, because the code is publicly vetted (other apps like Telegram have not had external vetting to confirm if they are safe). WhatsApp will hand over information to law enforcement about who is in a particular group, while Signal does not. While vetting any information-sharing app, make sure to check if the audits are public and what their policies are in terms of legal cooperation. Always turn on 'Disappearing Messages' so messages self destruct. Finally, consider putting an additional pin lock on the signal lock itself. You can find a guide for app pin locks for [iPhone here](#) and for [Android here](#).
8. **Get a safety squad together.** If you are specifically under threat because you have been or are likely to be doxxed, set up a check-in plan where you call or text someone at a set time every day or at set intervals, and have a plan for what to do if you don't make the check-in (like call an attorney, go check at your house, etcetera). Consider having a backup place to stay, like a friend's house

WHAT TO PACK

- **Fully charge battery backup with correct cables** - This is useful for phones or other devices you may need to power.
- **A Sharpie pen and notepad** - You will need this to write down vital information, like legal hotline numbers. Write down emergency phone numbers to contact in case of arrest or detention.

PHONES

- **If you are considering participating in diversity of tactics or getting arrested, consider leaving your phone at home. YOU ARE BEING GEOTRACKED.**
- **Download and start using [Signal Messenger](#) on your phone.** Make sure all your comrades also have it and are using it.
- **If you can't leave your phone at home,** you can either purchase a Faraday bag, which blocks signals from your phone, or [make your own](#). You can do that by **triple wrapping** your phone in aluminum foil tightly and make sure there are no holes. **Turn on airplane mode** or **turn off your phone** entirely. This quick and dirty method will block all signals going in and out of your phone, and can help thwart geolocation of you. It is not a foolproof method but it is a mitigation method.or

- **Enable an alphanumeric PIN code on your phone, that is at least 10 characters long,** to prevent police or thieves from getting into your phone. **DO NOT use facial recognition or thumbprint unlock. DO NOT use a low digit PIN code** as they can be cracked. Most recent phones allow you to take photos and film even with the PIN lock. Keep in mind that police cannot (legally) force you to unlock your phone. If your phone model is an older one, turn on the encryption feature.
- **If you are planning to use your phone to document the protest check out the [Witness guide](#)** to safely filming during protests. These tips will assist you in ensuring that you film safely and use your footage ethically

KNOW YOUR SUPPORT

- **Find a buddy:** Protests sites are dangerous. Always make sure you go out with a friend who can help you through a situation.
- **If anticipating arrest:** Find and write down your state's local [National Lawyers Guild hotline number](#) on your arm with a Sharpie, in case of arrest.

COMMUNICATIONS

1. **DO NOT UPLOAD EASILY IDENTIFIABLE IMAGES TO SOCIAL MEDIA.**- Beware of **faces** and **tattoos** in particular. White supremacists and law enforcement will comb through these posts and try to reverse identify people. Please see [this guide](#) for a checklist of responsible video practices.
2. **DO NOT POST ILLEGAL ACTIVITY OF YOU OR FELLOW PROTESTORS TO SOCIAL MEDIA. ASK YOUR FRIENDS TO NOT TAG YOU.** Police and trolls will use public social media posts to do their work.
3. **Use Signal Messenger ONLY at all times with disappearing message timers. DO NOT USE TEXT MESSAGING, PHONE CALLS, EMAIL, WHATSAPP, or FB MESSENGER.** Police investigations often will only look at the people you are communicating with and not the content of messages as the former does not require a warrant. Signal is an application that is proven to effectively hide your call and messaging history. Please use [this guide](#).

IN CASE OF ARREST

- **Do not give out PIN code, passwords, or other bits of useful information to the police.** If your phone is compromised to the police, your entire community is effectively compromised. If police ask, tell them that you refuse consent to a search of your devices.
- **Remain silent. Ask for a lawyer** for any and all questions.

AFTER THE ACTION

- **If you are facing doxxing, trolling, or harassment**, please refer to [this guide](#), and contact Equality Labs or any other digital security team that has expertise in countering doxing.
- **Sanitize your data:** Police investigations may happen for months after protests. Sanitizing and flushing your data will help protect you and your network. There is no guarantee that platforms will not produce a backup copy at request, but deleting data is still a good start.

Google: Your data on Google servers may be used against you as time goes on. Potentially damaging data includes searches and geolocations. We recommend a best practice of deleting all your history. If you need a backup before you delete, go to [this link](#) and store the backup on an encrypted USB drive. DO NOT store it on a cloud service.

1. On your computer, go to your **Google** Account.
2. On the top left navigation panel, click Data & personalization.
3. Under "**Activity** and timeline," click My **Activity**.
4. Find the group of **activity** you want to **delete**.
5. At the top of a group, choose More.
6. Click **Delete**.

Facebook: Delete conversations.

1. Click  in the top right of Facebook.
2. Open the conversation you want to delete.
3. Click  at the top of the chat window and select **Delete conversation**.
4. Click **Delete Conversation** to confirm **Signal**

Signal: Remove any sensitive signal threads.

1. Go to the conversation list.
2. Tap and hold a conversation.
3. Tap the outlined square to select all conversations.
4. Tap **Delete**.
5. Select **Delete** to confirm.

WhatsApp

1. Open **WhatsApp** and go to the chat containing the message you want to **delete**.
2. Tap and hold the message. Optionally, select more messages to **delete** multiple messages at once.
3. Tap **Delete** > **Delete for everyone**.

Secure Erasing Devices: You may need to think about wiping your laptop or phone clean. Many times, the "delete" feature does not actually remove the data, but rather keeps it in a special area to be

recycled. Use a secure wipe application to truly remove the data and make it difficult for forensics to retrieve:

1. **Android and IOS:** use an app like [iShredder](#)
2. **Mac:**
 - a. Make sure your Mac is turned off.
 - b. Press the power button.
 - c. Immediately hold down the **command** and **R** keys.
 - d. Wait until the Apple logo appears.
 - e. Select "Disk Utility" from the OS X Utilities list. Click **Continue**.
 - f. Select the disk you'd like to erase by clicking on it in the sidebar.
 - g. Click the **Erase** button.
 - h. Click the **Security Options** button.
 - i. The Security Options window includes a slider that enables you to determine how thoroughly you want to erase your hard drive.
3. **Windows:** [Eraser](#) is a free tool that will allow you to securely delete Windows data.

Practice Self-Care

We are grieving and exercising courage for the collective liberation of our people. Participating in these protests and the pain of this moment means we are moving through trauma. Here are [Healing Justice resources from the Movement for Black Lives](#). We encourage you to seek out whatever can help replenish and soothe this pain for you as well. This could include Black healing circles, therapists, and even altar work. We are here for each other and this includes holding each other's grief as we fight for a world where we exist beyond this violence.